# Proof of Concept (POC) Documentation

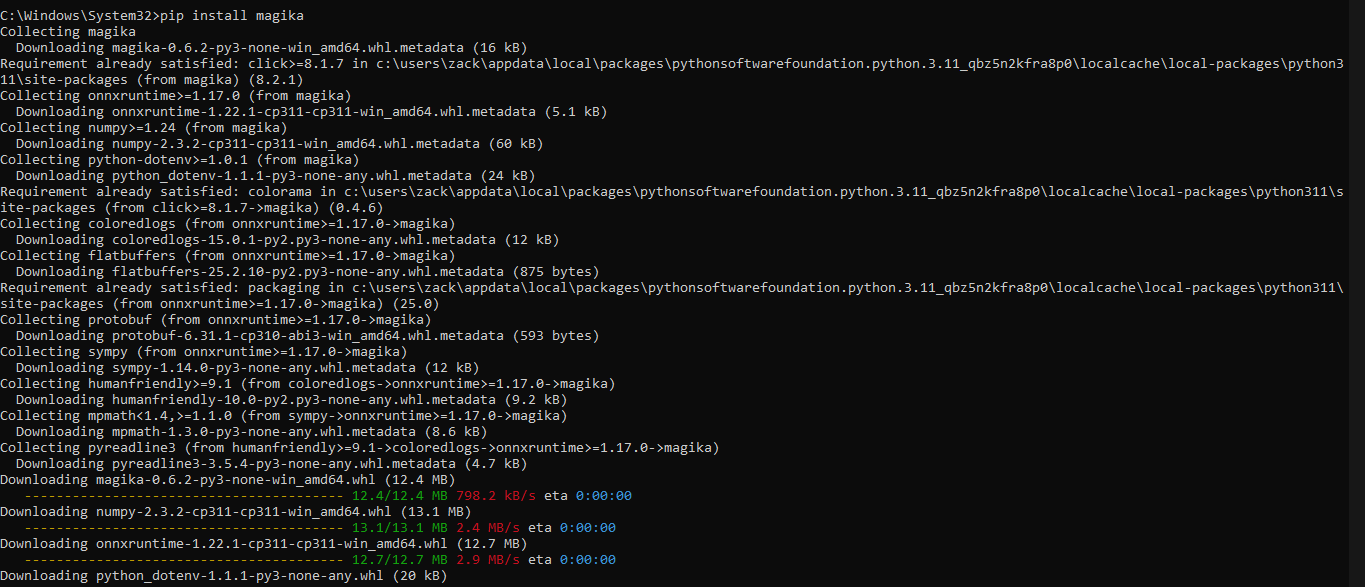
**Project Title:** Magika & Malware-Jail Malware Analysis Tools

**Name:** Riya Bhutal  
**Intern ID:** 248  
**Date:** 25-07-2025

### **Objective:**

To demonstrate the installation, configuration, and basic usage of **Magika** and **Malware-Jail**, which are tools used in static and dynamic malware analysis respectively.

### **1. Magika: File Type Detection Tool:**



**Description:**  
Magika is a machine-learning-based file type identification tool developed by Google. It helps identify file types in a more intelligent way than traditional methods like file command or magic numbers.

**Installation:**

pip install magika

**Usage Example:**

magika sample.exe

**Expected Output:**

The tool will return the predicted file type of sample.exe, such as:

sample.exe: PE32 executable (Windows executable)

**Use Case:** Magika helps triage malware samples by determining the file type accurately, even in the presence of obfuscation or incorrect extensions.

### Hybrid Detection of Malicious Portable Document Format (PDFs): Safeguarding Against Embedded JavaScript Attacks | SpringerLink**2. Malware-Jail:**

**Description:**  
Malware-Jail is a sandbox tool for emulating Windows malware behavior using a JavaScript-based environment. It can simulate Windows APIs and help in safe, static/dynamic behavioral analysis.

**Installation:**

1. Clone the repository:

git clone https://github.com/bontchev/malware-jail.git  
cd malware-jail

1. Run the main script using Node.js:

node jail.js <malware\_script.js>

**Example:**

node jail.js test/in/peb.js

**Expected Output:**  
The tool simulates how the JavaScript-based malware interacts with Windows APIs and shows the emulated output.

**Use Case:** Malware-Jail is helpful when analyzing JavaScript malware or scripts that target Windows environments. It prevents the malware from affecting the analyst’s actual system.

### 

### **Safety Guidelines:**

* Always run tools in a controlled and isolated environment (e.g., virtual machine).
* Never open actual malware samples on your main host OS.
* Do not connect the sandbox environment to the internet during analysis.

### **Conclusion:**

Magika and Malware-Jail are effective tools in the malware analysis workflow. Magika aids in accurate file type detection, while Malware-Jail offers a lightweight dynamic analysis sandbox for script-based malware.